Q. P. Code: 27400

Time: 3 hours

Marks: 80

1. Q.1 is **compulsory**.
2. Attempt any **three** questions from the remaining **five** questions.

Q.1 (a) Discuss the concept of LZ78 with an example. (5)

(b) What is motion estimation? How is it useful for video compression? (5)

(c) Define Euler's totient function. Compute $\Phi(37)$, $\Phi(49)$, $\Phi(100)$. (5)

(d) Define hash function and state its properties. (5)

Q.2 (a) Consider a source with symbols = {m, n, o, p} with corresponding probabilities {0.4, 0.3, 0.1, 0.2}. Using arithmetic coding, determine the output tag for the message "mnnop". Also, reconstruct the message using this tag. (10)

(b) Draw and explain the working of AES encryption algorithm. (10)

Q.3 (a) Using RSA algorithm, user X chooses the public key ($n = 21$, $e = 5$). Compute the private key d of user X. (10)

User Y wants to transmit message $M = 19$ to user X in a confidential manner using RSA algorithm; determine the cipher text C.

(b) Draw and explain the working of JPEG image compression standard. (10)

Q.4 (a) Discuss the concept of μ-law companding. Using μ-law companding, determine the encoded output value for an input audio sample with value (+358). Also, reconstruct to determine the decoded value. (10)

(b) What is Certificate Authority? How is a digital certificate obtained and verified? (10)

Q.5 (a) What is Intrusion Detection System? Discuss the different techniques of implementing it. (10)

(b) Solve the linear congruent equation for x: $232x + 42 \equiv 48 \bmod 50$. (5)

(c) How is the accumulation of error avoided when using DPCM for image compression? (5)

Q.6 (a) Draw and explain the working of Key Distribution Center for exchanging secret keys. (10)

(b) Compare statistical and dictionary compression techniques. (5)

(c) What is a one-way trapdoor function? List three one-way trapdoor functions used in cryptography. (5)

****